ABSTRACT OF THE DISCLOSURE

In a network having hierarchical domain names and a DNS server for managing the correspondence between the domain name and the address located at each hierarchy, each DNS server provides a module for managing a public key and a database for indicating correspondence between a public key and a domain name of the host belonging to the network. When two hosts start to do security communication with each other, one host operates to automatically acquire a public key of a target host from the function-expanded DNS. The packet for inquiring the public key contains the name of the DNS server trusted by the host. The DNS server specified by this host operates to add an electronic signature to the packet for answering the public key. The host enables to determine if the public key contained in the packet for answering the public key may be trusted on this electronic signature, thereby preventing a malignant host from feigning be a target host.